Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

Microsoft

Upcoming negotiations on a possible cybercrime convention

Microsoft's submission

Cybercriminals have proven themselves to be skilled and relentless. Experience shows they have been able to continuously evolve and increase their sophistication, employing methods that make them harder to detect and threatening even the most well-prepared targets. They do not respect international borders and tend to hide in jurisdictions that do not have the legal frameworks that would allow for their prosecution, that lack the capability to track them down, that tacitly support the activities, or that simply have no interest in the cross-border cooperation needed to contain this global threat.

The recently published Microsoft Digital Defense Report draws on insights, data, and the trillions of signals from across the company's platforms, including the cloud, endpoints, and the intelligent edge[1]. The conclusions of the report are sobering. Over the past year the world has borne witness to a burgeoning cybercrime economy and the rapid rise of cybercrime services – against an already high baseline. We have watched this global market grow in both complexity and fervency. We have seen the cyberattack landscape become increasingly sophisticated as cybercriminals continue, and even escalate, their activity in times of crisis. New levels of supply chain and ransomware attacks were a powerful reminder that all stakeholders must work together, and in new ways, to protect the cybersecurity of the planet.

Despite increasing investments and regulatory focus on cybersecurity, much more clearly needs to be done to address this threat. This includes investments in and implementation of effective cybersecurity practices, capacity building efforts to ensure cybercriminals can be brought to justice no matter where in the world they are operating from, as well as legal and technical innovation to keep up with the creativity malicious actors are demonstrating. Indeed, Microsoft does not believe that a new cybercrime convention will provide all the answers and would prefer for the international community of states to focus instead on implementing and evolving existing agreements that enable international cooperation to combat cybercrime. However, given that negotiations on a new cybercrime convention are proceeding, we do think that, appropriately scoped, it can provide a useful tool to streamline cross-border cooperation to bring the fight to the criminals. To do so, it is important that any instrument that is adopted does not undermine existing tools and processes, such as the Convention on Cybercrime of the Council of Europe (the Budapest Convention)[2], but focuses instead on enhancing cooperation exclusively for combatting cybercrimes.

Microsoft urges states to avoid using this negotiation as a catch-all framework to discuss other topics, such as extremism and terrorism. This is not to diminish the significance of these or other such issues, simply to recognize that they have been and are more appropriately addressed elsewhere than in a cybercrime treaty. Similarly, we believe the convention should not be a vehicle to drive content regulation or attempt to merge this process with the discussions taking place in the United Nations First Committee relate to international security and responsible state behavior in cyberspace. Undermining or replacing those or other existing agreements will do nothing to address cybercrime and will instead drive a wedge between different international efforts. Alternatively, a new convention should pursue a focused scope and work to establish an effective set of remedies for those crimes.

Moreover, a new cybercrime convention cannot become an avenue for states to remove or shirk their existing obligations under international law, especially international human rights law. Its primary purpose should be

[1] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

[2] https://www.coe.int/en/web/cybercrime/the-budapest-convention

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

to protect the targets and victims of cybercrime rather than provide a pretext for non-democratic regimes to further endanger the free and open internet by closing off their digital borders. In the past, some governments have abused cybercrime measures, using domestic cybercrime legislation to criminalize the publication and dissemination of unwelcome content online, to impose mass digital surveillance, and to curb the right to privacy in the name of fighting terrorism. A new treaty should remove the opportunity for this behavior in its design. Instead, a new convention should add to or streamline existing international legal obligations with a focus on protecting victims and ensuring a free and open internet.

In the recommendations that follow, we address these points under three different headings that reflect the different aspects of the upcoming negotiations: 1) the negotiating process, 2) objectives that should guide the negotiation, and 3) the potential scope of a convention.

Process

The negotiation process will require full transparency and multistakeholder engagement if they are to be successful and any resulting treaty meaningful. Cyberspace is developed and maintained by many actors from different sectors around the world. They all bring different experiences, resources and approaches to the table. For example, the technology sector operates much of the infrastructure on which attacks by cybercriminals are being executed, and as a result has the greatest insight into the techniques and tools being used, as well as data and information that might help hold malicious actors accountable. In short, the inclusion of different stakeholders is critical because the challenges the world faces in addressing cybercrime are such that no single actor is in a position to mitigate, let alone resolve, them alone. With that in mind, Microsoft urges states engaging in the upcoming negotiations on a new cybercrime treaty to:

- Pursue a **systematic multistakeholder approach** through meaningful inclusion and consideration of the equities of civil society, industry, academics, technical experts, and scientific and research institutions. They should be able to participate in the negotiations to the fullest extent possible – this includes observing meetings and providing regular written and in-person contributions to the negotiations throughout. Furthermore, individual states should pursue consultations with the multistakeholder community outside the formal Ad Hoc Committee processes. While ultimate decision making power will always remain with states, multistakeholder voices and expertise must be included to support states in making the best possible decisions.
- **Promote transparency** so that the negotiations are as open as possible. This includes the sharing of schedules, participants and draft texts, all of which should be made available to the public. Relatedly, all relevant stakeholders should be empowered to provide written proposals to the consultation, in a systematic manner.
- **Ensure widespread adoption** by adopting a consensus-based approach at the center of the negotiating process, and by setting a high standard in terms of ratifications required for the convention's entry into force. This will ensure that any new instrument does not unintentionally fragment the online environment further.

Objectives

For negotiations to be successful, all parties must be aligned on a concrete set of objectives. It is important to recognize from the outset that the states participating in the negotiations face different challenges in cyberspace and also bring diverse cultural and legal frameworks to the table. In this environment, consensus can be difficult to achieve. Nevertheless, consensus is essential as a new convention will only be effective if it enables the widest possible international cooperation, which requires a broad global coalition. As such, there must be alignment around a clear and focused set of objectives.

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

The primary purpose of any new convention should be to combat cybercrime (narrowly defined, as per the next section) while prioritizing human-centric equities. Effectively applying existing solutions to enforce international cooperation between the judiciary and law enforcement under transparent oversight, while respecting human rights, should be the cornerstone of the new treaty. With that in mind, Microsoft hopes the following objectives will guide the negotiations:

- A new convention should encourage **effective international cooperation** between national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime. It should draw upon existing treaties and include options for refusal on the grounds of dual criminality, refusal in respect of political offences, and refusal of a request made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender, or other protected characteristics. As outlined in our overall comments above, we encourage negotiators to seek to ensure that human rights protections are clearly factored in at every step of the negotiations, and that rights to free expression, access to information and privacy are preserved in line with certain minimum standards of proportionality and necessity.
- A new convention provides an opportunity for greater collaboration between governments and the private sector in matters related to **lawful data access**. This is especially the case for cloud service providers. States should use this opportunity to recognize the need to resolve any existing conflicts of laws, jurisdictional and sovereignty issues in this space. Moreover, any lawful data access framework needs to include the requirement that access to digital information is only allowed pursuant to lawful process and create an opportunity for technology providers to challenge such process on behalf of their customers to ensure that governments are acting within the law and are respecting the rights of their users. Moreover, except in limited cases, individuals and organizations have a right to know when governments access their digital information. Secrecy should be the exception not the rule.
- A new convention should also provide a **framework for capacity building** to enable the effective investigation and prosecution of cybercrime globally**.** Today, countries are at vastly different levels of readiness when it comes to cybercrime investigation and prosecution. Work is needed to empower authorities to prevent and counter cybercrime irrespective of where they are in the world, as criminals continuously evolve and adapt their tactics. We therefore hope that a new convention will provide a framework for training programs in this area, as well as technical assistance that could support the implementation of the convention.
- A new convention should ensure **ongoing consultations with the expert community.** While we urge states to ensure that the convention is time-proofed and any definitions are technology neutral, we recognize that this is a fast-evolving environment. The creation of an expert forum that would allow states and participants from technical communities and industry to exchange views on the latest threats and potential mitigations would add to the security and stability of the online environment.

Scope

As mentioned at the outset, Microsoft believes that negotiations will only be successful, and any resulting convention only effective, if its scope is narrowly defined. Acts of cybercrime, more often than not, cross borders and so international cooperation is therefore at the core of effective prosecution. However, this kind of cooperation requires that the offences included are commonly understood and recognized by all parties involved. With that in mind, we encourage states to:

- **Criminalize substantive offences that are cyber-dependent**; e.g. illegal access; however only do so when description and definitions are widely accepted. A focus on serious crime would also be welcome to help streamline the processes and procedures.

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- **Do not duplicate offences** that are covered by other legal instruments, such as corruption, trafficking or terrorism simply because these may be complemented using information and communication technologies. Such an approach risks contradiction and confusion and will not deliver a targeted, practical instrument that can improve the collective ability to tackle cybercrime.
- While Microsoft appreciates the need to address novel and emerging forms of cybercrime, we strongly urge caution in relation to including any "cybercrimes" that are **focused on online content**, given some of the particular human rights challenges that content-related crimes can and have raised in other contexts. States should specifically avoid any commitments that would result in preventive content take downs.
- **Do not to treat traditional crimes as cybercrime in a new treaty** merely because a computer was involved in the planning or execution of the crime. These types of activities can generally be covered by other statutes. These types of offenses should only be included where the scale, scope, or speed of the offense is significantly increased by the use of the Internet, and where the definitions are commonly understood, for example as it relates to child sexual exploitation.
- Finally, in addition to the criminalization of substantive offenses, we believe any new convention should address the need for domestic legal authorities to **preserve, collect, and share electronic evidence**, consistent with due process and the protection of human rights and fundamental freedoms. Specialized procedural authorities to collect electronic evidence are essential in ensuring international criminal investigations.

We hope these recommendations provide a helpful contribution to advance a shared objective: achieving a rules-based and rights-respecting online world for all. More than anything else, we believe accomplishing this requires trust and cooperation across stakeholder groups with responsibilities in this space. Please let us know if we can provide any additional input or clarify any of the contributions provided here and we look forward to additional opportunities to collaborate in the future.